While you wait...

Why not let us know what topics you'd like us to cover next?

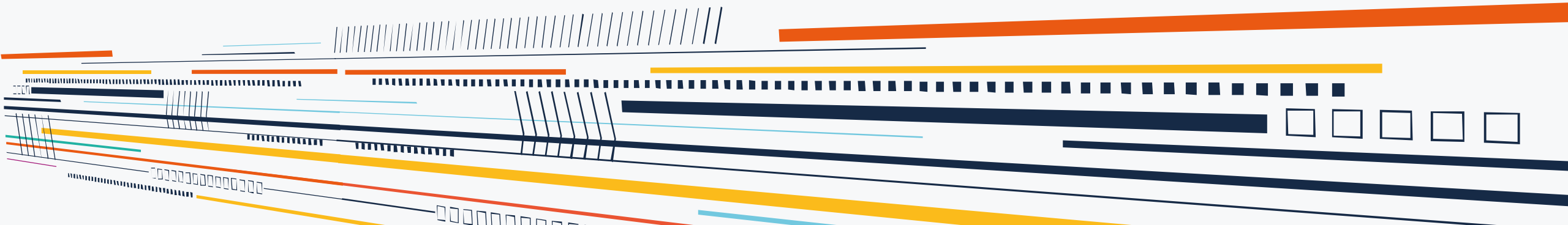
Take the short survey at:

squaredup.com/topics

SquaredUp

Coffee Break Webinar Series

Community MPs (Experts Live)



Topic

Community MPs

Discussion points:

- Experts Live recap
- PowerShell Monitoring MP
- SQL Query MP
- Security Monitoring MP
- SCOM Web API
- OMS Administration MPs

Experts Live

- 3 days of System Center, Azure and IT management content in Berlin, Germany
- Almost 400 people from 28 different countries
- 50+ presenting experts, 31 of them Microsoft MVPs
- 16 sponsors
- 100 sessions in 6 parallel tracks

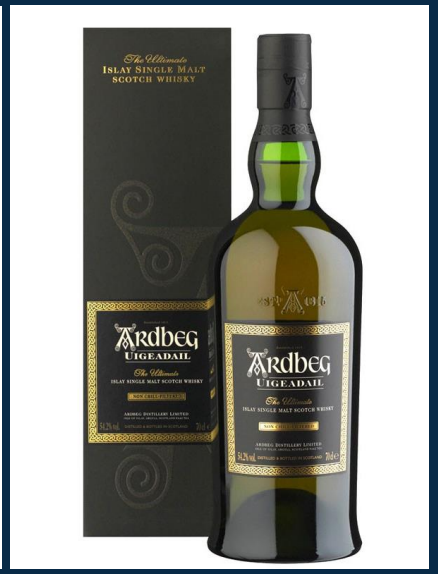
SCOM/OMS Sessions:

- Kevin Greene – Monitoring… the next generation
- Richard Benwell – Whisky and Community MPs
- Christian Heitkamp – SCOM Tips and Tricks
- Alexey Baltikov – OMS Query Language
- Marcel Zehner – Creating custom OMS Solutions

Upcoming events in USA, APAC, Australia

http://www.expertslive.eu/experts-live-network.html

SCOM Community + Whisky

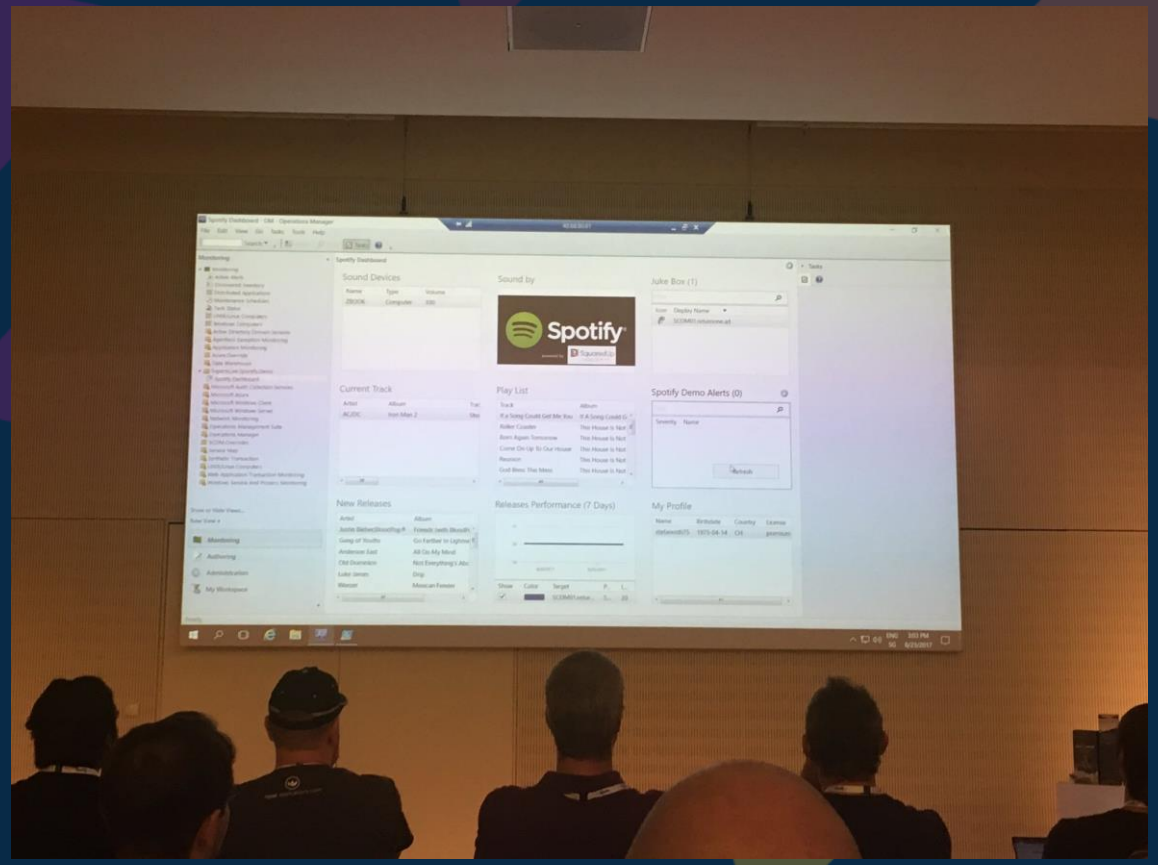


PowerShell Monitoring MP

https://squaredup.com/free-powershell-management-pack/

Free, open source MP that adds PowerShell support to SCOM

Stefan Roth showed us how to use it for Spotify integration with SCOM!



PowerShell Monitoring MP

Squared Up competition to suggest uses of the PowerShell MP

Lucky winner of the Lego Death Star is Christian Schmidt

Agent task to determine missing updates, download and install from SCCM Software Center

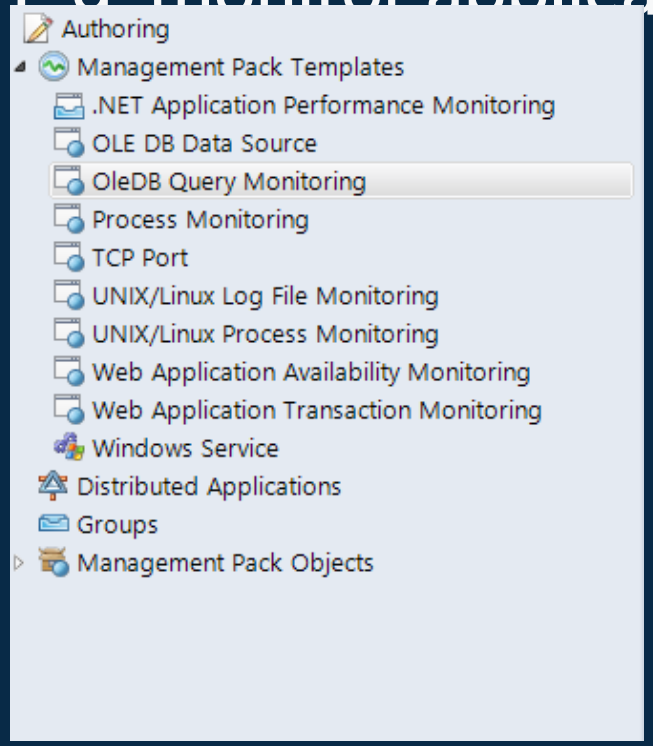
```
$MissingUpdates = Get-WmiObject -Class CCM_SoftwareUpdate -Filter ComplianceState=0 -
Namespace root\CCM\ClientSDK

$MissingUpdatesReformatted = @($MissingUpdates | ForEach-Object {if($_.ComplianceState -eq
0){[WMI]$_.__PATH}})

$InstallReturn = Invoke-WmiMethod -Class CCM_SoftwareUpdatesManager -Name InstallUpdates -
ArgumentList (,$MissingUpdatesReformatted) -Namespace root\ccm\clientsdk
```

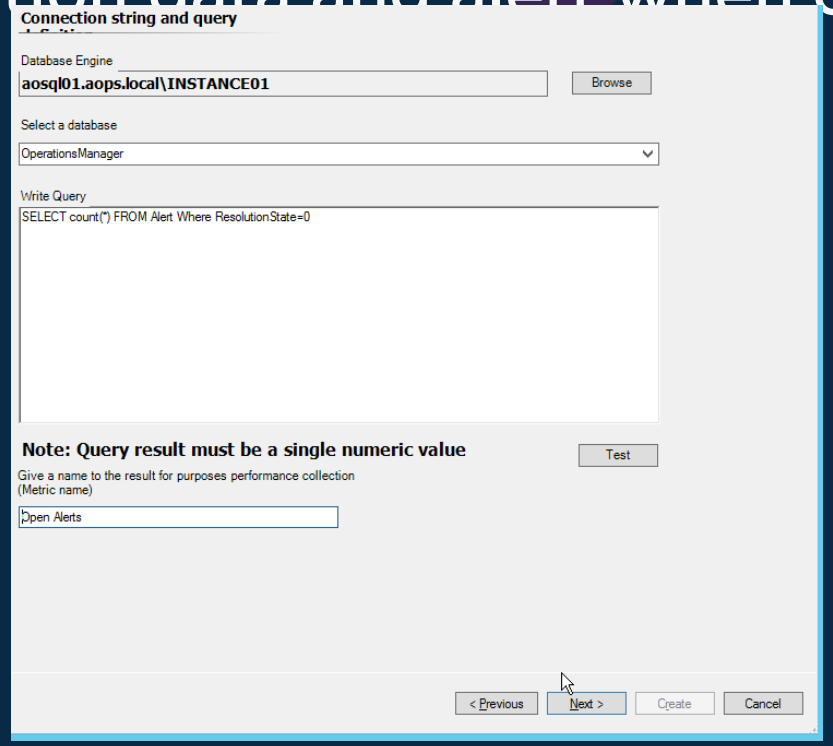
OLE DB Query Monitor MP

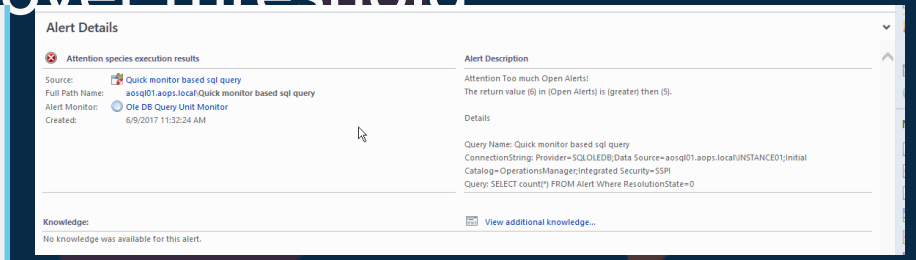
https://github.com/UretzkyZvi/Monitor-Applications-Using-SQL-Queries

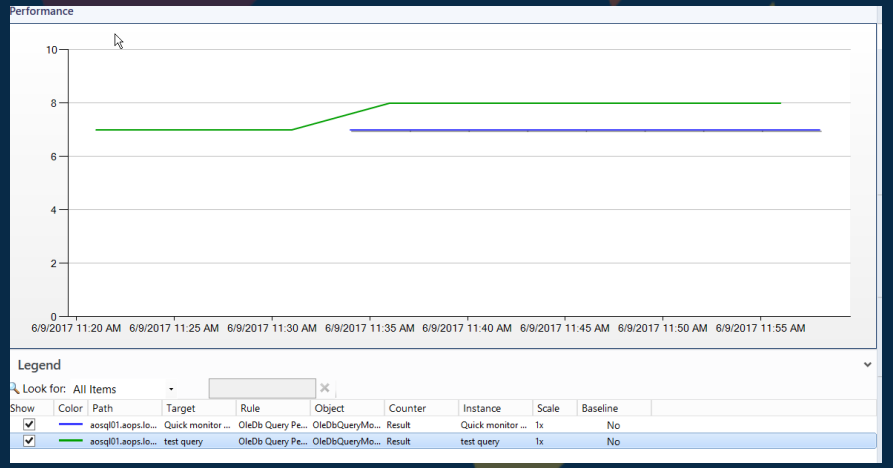
Create SCOM monitors from any SQL query

E.g. monitor application data and alert when over threshold









Security Monitoring MP

https://blogs.technet.microsoft.com/nathangau/2017/05/01/introducing-the-security-monitoring-management-pack-for-scom

"I'm not sure on the latest statistics, but at that time it was noted than attacker is in an organization on average for about 250 days before they are found"

"Organizations that prioritize security spend large amounts of money on big data tools like Splunk or OMS in conjunction with SCOM and Azure PowerBI, but these take an extensive time investment, training, and in some cases rare resources, and that's before considering that you actually have to know what you're looking for. " – Nathan Gau

Domain Admin, Enterprise Admin, and Schema Admin Group change monitoring
Pass the hash, overpass the hash, and pass the ticket detection
Detect the creation of a service on a domain controller
Local Admin Group modified on member server
Scheduled task creation
Software was installed on a server
Software was removed from a server
System was powered off
Kevin Holman's failed RDP attempts monitor
System pending restart monitor
Loads more…

SCOM Web API

https://github.com/ehrnst/System-Center-Operations-Manager-API

"Make SCOM accessible to your millennial developers" – Martin Ehrnst

Simple IIS website installed on the SCOM management server that provides a SCOM REST API.

E.g.

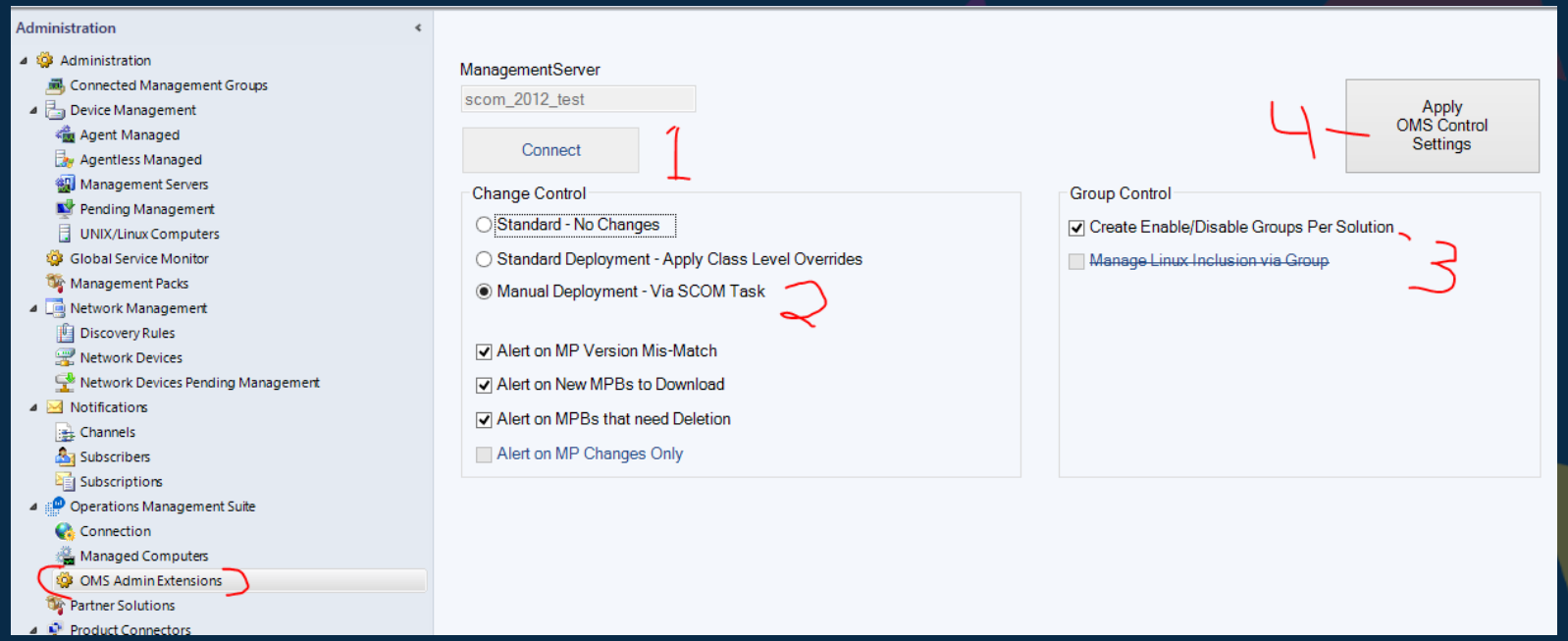
```
[GET] http://mgmtsrv1/API/Alert/{id}
[POST] http://mgmtsrv1/API/ObjectMaintenance
```

OMS Administration MPs

https://github.com/P2P-Nathan/OMS-Administration-Packs

Be in control of your OMS solutions (and costs!)

- Which agents get which solutions
- Gatekeeper for when OMS updates get deployed into production



Coffee Break: Resources

Let us know what you'd like us to cover:
squaredup.com/topics

See what's coming up next:
squaredup.com/coffee-break-series

Recordings and slides published via
squaredup.com/blog

YouTube playlist for series
https://www.youtube.com/playlist?list=PLJNXoiGgmTEu3yZRGpPNWQbG9WMyihZFs

Follow up email, inc. resources, sent out after each webinar

Q&A